REMARKS

Claims 1, 3-10, 12-15, 17-25, 27-30, and 39-47 are pending in this application. By this Response, claim 9 is amended and claims 39-47 have been added. Claim 9 is amended to correct a typographical error. Claims 39-47 are added to recite additional features of the present invention. Support for the subject matter recited in claims 39-47 may be found at least in Figure 1 of the present specification and on page 16, lines 1-10. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Telephone Interview

Applicant thanks Examiner Klimach for the courtesies extended to Applicant's representative during the April 13, 2006 telephone interview. During the telephone interview, the distinctions of the present claims over the alleged combination of Khoda, Yu-Huang, and Schneier were discussed. Examiner Klimach agreed that the claims appear to overcome the alleged combinations of references because Yu-Huang does not appear to teach or suggest the feature of "in the decryption of data, if a data item is skipped and not received, the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result" as recited in claim 1 and similar features found in the other independent claims. Examiner Klimach stated that she needed to review the Yu-Huang reference again in more detail before making a final determination and requested that Applicant's representative submit arguments in writing. The substance of the telephone interview is summarized in the following remarks.

II. Request for Initialed PTO Form 1449

An Information Disclosure Statement and PTO Form 1449 were filed with the present application on February 14, 2002. Applicant has not received a copy of the initialed PTO Form 1449 indicating consideration of the references by the Examiner. Thus, Applicants respectfully request that the Examiner forward a copy of the initialed PTO Form 1449 along with the next communication from the U.S. Patent and Trademark

Office. For the convenience of the Examiner, a copy of the originally filed PTO Form 1449 is attached hereto.

III. Rejection under 35 U.S.C. § 103(a) Based on Kohda and Yu-Huang

The Office Action rejects claims 1, 3, 5-10, 12-15, 17, 19-25, and 27-30 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Kohda et al. (U.S. Patent No. 6,014,445) in view of the article by Yu-Huang et al. entitled "Dynamic data encryption system based on synchronized chaotic systems." This rejection is respectfully traversed.

Claim 1, which is representative of the other rejected independent claims 15 and 30 with regard to similarly recited subject matter, reads as follows:

> 1. A method of encryption and decryption of data, in which the data is made up of a series of data items, the method including the following steps:
>
> selecting a chaotic equation;
>
> defining starting conditions of the variables of the chaotic equation in the form of an input key; and
>
> <u>applying the chaotic equation to each data item, wherein the method includes an iterate step of updating the chaotic equation and the input key for each iteration value and, in the decryption of data, if a data item is skipped and not received, the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result.</u> (emphasis added)

Neither Kohda nor Yu-Huang, either alone or in combination, teach or suggest the emphasized features above. Kohda is directed to an enciphering/deciphering apparatus and method incorporating a random variable and keystream. With the mechanism of Kohda, a chaos generation means generates a real-valued sequence along a chaotic orbit in accordance with a predetermined number of first common keys and a predetermined nonlinear map. A bit generation means performs a predetermined binarization on each real value in the generated real-valued sequence based on a predetermined number of second common keys to generate a binary sequence. A logic operation means executes a predetermined logic operation on a binary sequence of an input plaintext and the generated keystream sequence bit by bit to generate a binary sequence of a ciphertext.

Kohda teaches in Figures 4 and 5 and the corresponding text at column 18, lines 23-60 that the chaos generator has a feedback loop in which the output real value ωn-1 is fed back into the non-linear map for generating a series of real values that are provided to a threshold function in a bit generator to thereby generate the keystream.

From the above, it is clear that, with the mechanism of Kohda, a real-valued sequence is generated by a chaos generation means based on first common keys. A binarization on the real values is generated based on second common keys, and a logic operation is performed on binary sequence of input plaintext and the generated keystream to generate ciphertext. Nowhere in Kohda is there any teaching or suggestion that, in the decryption of data, if a data item is skipped and not received, the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result. The Office Action admits that Kohda does not teach these features (see Office Action, page 3, first full paragraph), but instead relies on the article by Yu-Huang as allegedly teaching these features.

Yu-Huang teaches a dynamic data encryption system for use in secure communication systems. In the system, the waveform for each n encrypted bits is mapped to one of 2^n distinct arbitrary chaotic dynamic equations. Essentially, as described on page 272 of Yu-Huang, a plurality of chaotic attractors functions $f_i(x_i,p_i)$ are provided that generate information signals x_1-x_m, where $i=1...m$. These information signals are provided to an encoder which encodes the information signals using generator functions $h_i(x_i)$ that generate driver signals. Every period T, one of the information signals x_i is selected from one of the 2^n chaotic attractors and, as a result, one of the driver signals r_1-r_m is selected for output to generate the output signal s.

On the other end, at the decryptor, the output signal s is received and input to a plurality of response chaotic attractors $f_i'(y_i, p_i, s)$ which generate outputs that are operated on by the driver signal generator functions to generate a plurality of outputs to a optimal decision rule unit. The optimal decision rule unit compares the difference between the input signals to the optimal decision rule unit and the original input s to the response chaotic attractors. The minimum difference is selected as the information signal x_i that was sent by the encryptor. This encryption/decryption operation is performed for each n number of bits.

Yu-Huang does not teach or suggest that, in the decryption of data, if a data item is skipped and not received, the iterate step of the chaotic equation is applied for the skipped data item and the result is discarded. The Office Action alleges that this feature of claim 1 is taught by Yu-Huang at paragraph 3 of the second column on page 272, which reads as follows:

> *Conclusion*: We have proposed a novel chaotic digital communication system. This system can prevent intruders from recovering the information signals. Moreover, in this method, each information signal is run separately in its own domain of attraction, so that there is no danger of divergence. In addition, each time a received signal is identified, is *n* bit representation can be determined. Hence, the speed is n times faster than chaotic switching methods. Finally, a modulator and demodulator can be implemented at each end of the transmission medium to increase the flexibility of the digital communication system.

From the above reproduction of paragraph 3, it is clear that there is nothing taught or suggested in this paragraph that speaks to skipped data items, applying an iterative step to a skipped data item, or discarding a result of the application of an iterative step of a chaotic equation to the skipped data item. Furthermore, nowhere else in Yu-Huang is there any teaching or suggestion regarding these features. To the contrary, Yu-Huang makes no mention what-so-ever regarding skipped data items, let alone applying an iterative step of a chaotic equation to a skipped data item and then discarding the result. Examiner Klimach indicator her agreement that Yu-Huang does not teach or suggest these features of independent claim 1 during the April 13, 2006 telephone interview.

Since neither reference teaches or suggests the above discussed features recited in claim 1, and the similar features found in the other independent claims 15 and 30, any alleged combination of the teachings of these references, even if such a combination were possible and one were somehow motivated to make such a combination, still would not result in the features of claims 1, 15 and 30 being taught or suggested. Thus, contrary to the allegations raised in the Office Action, Applicant respectfully submits that the alleged combination of references does not obviate the invention recited in claims 1, 15 and 30.

Moreover, it is not at all clear how the teachings of Yu-Huang would be combined with the teachings of Kohda. While both references appear to be within the

same technological area, i.e. encryption/decryption of data using chaotic attractors, the mechanisms of the two references are completely different in their operation. It is not clear how one of ordinary skill in the art would combine a system that generates a real-valued sequence along a chaotic orbit, performs binarization on each real value in the generated real-valued sequence based on a predetermined number of second common keys to generate a binary sequence, and then executes a predetermined logic operation on a binary sequence of an input plaintext and the generated keystream sequence bit by bit, as recited in Kohda, with a system that utilizes a plurality of chaotic attractors, a plurality of driver signal generators, etc., as recited in Yu-Huang. Moreover, it is less apparent how one of ordinary skill in the art would combine and modify such systems in the particular manner that would be necessary to arrive at the invention as recited in claims 1, 15 and 30.

Furthermore, it is even less clear where there is any suggestion to make such a combination and modification in either of the references. Neither reference teaches or suggests a desirability to combine its teachings with the teachings of the other reference. In other words, there is no deficiency stated or implied in either reference for which the other reference is a solution. The only suggestion to even attempt to combine the teachings of the references is predicated on a prior knowledge of Applicant's claimed invention and the sole purpose of trying to recreate Applicant's claimed invention having first had benefit of Applicant's disclosure. This is impermissible hindsight reconstruction using Applicant's own disclosure as a guide and is an improper basis upon which to make a rejection under 35 U.S.C. § 103(a).

Thus, in view of the above, Applicants respectfully submit that neither Kohda nor Yu-Huang, either alone or in combination, teach or suggest the features of independent claims 1, 15 and 30. At least by virtue of their dependency on claims 1 and 15, neither Kohda nor Yu-Huang, either alone or in combination, teach or suggest the features of dependent claims 3, 5-10, 12-14, 17, 19-25, and 27-29. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1, 3, 5-10, 12-15, 17, 19-25, and 27-30 under 35 U.S.C. § 103(a).

In addition to the above, dependent claims 3, 5-10, 12-14, 17, 19-25 and 27-29 recite additional features that are not taught or suggested by the alleged combination of

references. For example, with regard to claims 3 and 17, the Office Action alleges that Yu-Huang teaches that an updated chaotic equation is applied to each subsequent data item, in Figure 1. Figure 1 of Yu-Huang is as follows:

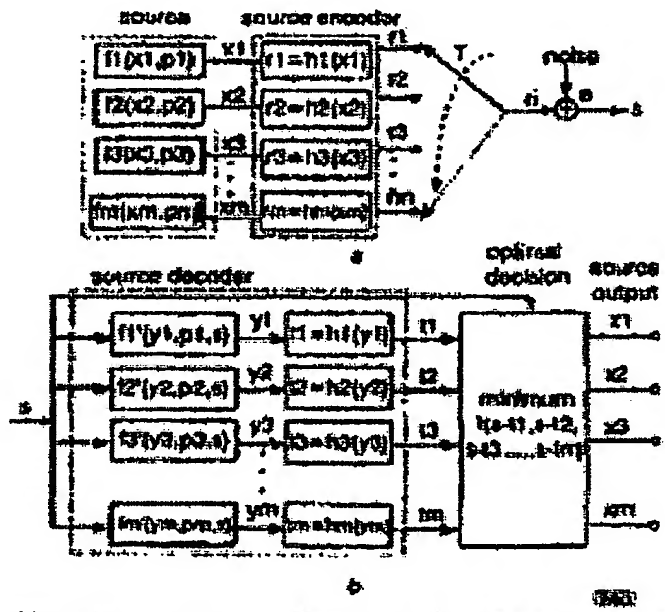

Fig. 1 Block diagram of secure chaotic digital communication system
a Transmitter
b Receiver

Nowhere in Yu-Huang is there any teaching or suggestion to actually update the chaotic attractors shown in Figure 1 or their input parameters. To the contrary, the same set of chaotic attractors are applied each time with a different chaotic attractor being selected for each period T. Thus, since nothing is updated in Yu-Huang, there is no possibility that an updated chaotic equation is applied to each subsequent data item, as recited in claims 3 and 17.

Moreover, Kohda does not teach or suggest these features either. While Kohda teaches a feedback loop in the chaos generator shown in Figure 4, this feedback loop is used as a means for updating the input to the non-linear map, thereby generating a keystream that is to be exclusively OR'd with the plaintext. Kohda does not iteratively apply the updated chaotic equation to each subsequent data item. To the contrary Kohda

generates a keystream sequence and then XOR's the keystream sequence with the plaintext to generate ciphertext, as shown in Figure 1 of Kohda.

As a further example, with regard to claims 5 and 19, the Office Action alleges that Yu-Huang teaches the feature of the encrypted data item being defined as v=(v xor |zn+1|)mod vmax, in Figure 1. From the reproduction above, it is clear that nowhere in Figure 1 of Yu-Huang is there any equation such as that recited in claims 5 and 19 shown or even implied in Figure 1 of Yu-Huang. Thus, despite the allegations made by the Office Action, Figure 1 of Yu-Huang does not teach or even suggest the features of claims 5 and 19.

Furthermore, while Figure 1 of Kohda shows an XOR operation between the keystream sequence and the plaintext, there is no teaching or suggestion in Figure 1 of Kohda that the encrypted data item has the definition recited in Figures 5 and 19.

The other dependent claims recite other additional features which, when taken alone or in combination with the features of the independent claims from which they depend, are not taught or suggested by the alleged combination of references. Thus, dependent claims 3, 5-10, 12-14, 17, 19-25 and 27-29 are allowable over the alleged combination of references by virtue of the specific features recited in these claims in addition to being dependent upon claims 1 and 15, respectively.

IV. <u>Rejection under 35 U.S.C. § 103(a) Based on Kohda, Yu-Huang and Schneier</u>

The Office Action rejects claims 4 and 18 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Kohda, Yu-Huang, and further in view of Schneier's book <u>Applied Cryptography</u>. This rejection is respectfully traversed.

Initially, the rejection is improper because the Examiner has failed to furnish Applicant with a copy of the pertinent sections of the Schneier reference and has failed to list the Schneier reference as a reference on the PTO-Form 892 provided with the Office Action. Thus, Applicant is not able to determine whether the Schneier reference referred to by the Examiner is actually prior art or that the assertions the Examiner has made regarding the Schneier reference are valid or not. Applicant respectfully requests that the Examiner provide a copy of the pertinent sections of the Schneier reference to Applicant

in the next communication from the Patent and Trademark Office as well as list the Schneier reference on a PTO-892 indicating the publication information so that it can be determined whether Schneier is actually prior art.

However, assuming that the Examiner is correct that Schneier is prior art, *arguendo*, and assuming that the assertions the Examiner made in the Office Action about the Schneier reference teaching modular arithmetic in cryptographic systems on page 243 of Schneier, the alleged combination of Kohda, Yu-Huang, and Schneier still does not overcome the deficiencies noted above with regard to independent claims 1 and 15, from which claims 4 and 18 depend, respectively. Therefore, even if Schneier were to teach modular arithmetic being used in cryptographic systems and one were somehow motivated to combine Schneier in some way with Kohda and Yu-Huang, the result still would not be the invention as recited in claims 4 and 18 since none of the references, either alone or in combination, teach those features emphasized above with regard to claims 1 and 15.

Moreover, simply teaching the use of modular arithmetic in cryptographic systems, as Schneier allegedly teaches according to the Examiner, does not obviate the specific features recited in claims 4 and 18. Claims 4 and 18 recite applying a modular arithmetic operation <u>to combine the real and imaginary parts of the result of the chaotic equation and the data item</u>. Simply teaching modular arithmetic does not teach or suggest to use modular arithmetic "to combine the real and imaginary parts of the result of the chaotic equation and the data item," as recited in claims 4 and 18.

Moreover, it is not at all clear how the general teaching of modular arithmetic allegedly in Schneier, would be combined with the systems of Kohda and Yu-Huang so as "to combine the real and imaginary parts of the result of the chaotic equation and the data item. Neither Kohda nor Yu-Huang mention anything about combining real and imaginary parts of a result of a chaotic equation with a data item. Kohda teaches the use of an XOR operation to combine a keystream sequence with a plaintext, but does not teach or suggest combining real and imaginary parts of a result of a chaotic equation with a data item. Thus, it is not clear how one of ordinary skill in the art, presented only with Kohda and Yu-Huang which do not mention real and imaginary parts of a result of a chaotic equation being combined with a data item, and Schneier which allegedly teaches

modular arithmetic, would suddenly come to the conclusion that it would be obvious to modify Kohda and Yu-Huang to use modular arithmetic to combine the real and imaginary parts of a result of a chaotic equation with a data item. The only suggestion to even attempt such a thing would necessarily come from a prior knowledge of Applicant's claimed invention and the sole purpose of trying to recreate the claimed invention, thereby constituting impermissible hindsight reconstruction.

Thus, in view of the above, Applicant respectfully submits that neither Kohda, Yu-Huang, nor Schneier, either alone or in combination, teach or suggest the features of claims 4 and 18. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 4 and 18 under 35 U.S.C. § 103(a).

V. Newly Added Claims 39-47

Claims 39-47 are added to recite additional features of the present invention. Claims 39-47 are dependent from respective ones of claims 1, 15 and 30 and thus, are allowable over the alleged combination of references for the same reasons as stated above with regard to claims 1, 15 and 30. Moreover, claims 39-47 recite additional features that are not taught or suggested by any of the cited references, whether taken alone or in combination. Prompt and favorable consideration of claims 39-47 is respectfully requested.

VI. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: April 13, 2006

Stephen J Walder Jr

Stephen J. Walder, Jr.
Reg. No. 41,534
WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. Box 832745
Richardson, TX 75083
(214) 722-6419
ATTORNEY FOR APPLICANT

Attachment:
Copy of PTO Form 1449 filed 02/14/02